INTERPOL

OPENING ADDRESS

by

Jürgen Stock – INTERPOL Secretary General

COUNTERING CYBER AND FINANCIAL CRIME: A HIGH-LEVEL DIALOGUE FOR A NEW GOVERNANCE ARCHITECTURE

12 July 2017

Lyon, France

INTERPOL Present Meng,
Distinguished guests,
Dear law enforcement colleagues,
Ladies and gentlemen,

Good morning. I would like to join INTERPOL President Meng in welcoming all of you to this *High-Level Dialogue* here in Lyon, France.

For us at INTERPOL, today is a very unique opportunity – one of strategic importance as we gather a sample of global actors from both the private and public sector that play a key role in an increasingly interconnected world.

The landscapes we each operate in are changing every day. These landscapes are being shaped by new technological developments and driven by social, economic and political demands.

The most recent evolutions have been seen through the cyber-attacks that hit many across the world – indiscriminately targeting both public and private sectors.

To cite only two: the WannaCry and Petya malware attacks tested the vulnerabilities of our modern, digital societies by weaponizing our own tools of progress against us.

The dawn of the Internet is behind us and has brought with it an enhanced set of capabilities that include accelerated communication channels, whilst at the same time reducing geographic distances to practical irrelevance.

What has benefitted our societies has also served the ends of transnational crime. And we are only just beginning to witness the impact of the cyber component on the evolution of transnational crime.

Parallel to purely ‘cyber-dependent’ crimes such as malware attacks, ‘cyber-enabled’ crimes, including telecom fraud and scams among others, are emerging at an unprecedented scale and speed.

The serious risks impacting on the safety of our communities, businesses and economies is why today’s High-level Dialogue for a New Governance Architecture is so important.
It is in the context of cyber-enabled crime that this conference gathers representatives from three key global sectors: financial, telecommunications and law enforcement.
All of us are stakeholders in this threat and I believe we must work together if we are to effectively tackle cyber and financial crimes in the future.

Our objective is simple: build a bridge between international law enforcement and industry to better prevent and mitigate cyber-enabled threats in the future.

Why INTERPOL? INTERPOL as an idea is 100 years old and has grown to be the largest international police organization because our member countries gathered to fight a common cause – transnational crime.

INTERPOL remains successful, useful and relevant today, because law enforcement from 190 member countries continue to share a common purpose to successfully deliver on our mission for a safer world.

Things have changed in 100 years, but our purpose remains the same.

The widespread use of the Internet as an everyday commodity has reinforced the need for enhanced global security. It has now given rise to new threats that are now common to both the public and private sectors, and which now call for a modern collaboration framework.

The need to modernize our partnership model also means that old methods of fighting crime are no longer sufficient in this context – as seen, for example, in the area of cyber-enabled child sexual exploitation.

To effectively address this global threat against the most vulnerable in our communities, INTERPOL and Microsoft partnered to integrate photo DNA technology into our International Child Sexual Exploitation Database.

Alone, neither party could fight this crime due to the lack of resources and expertise for the former, or simply a lack of a mandate in the case of the latter. A joint approach – and global response was necessary.

This approach has been used in the automotive, cultural heritage and pharmaceutical sectors – whereby INTERPOL has served as the platform of choice that brings together experts and resource from private and public partners, resulting in an enhanced global security architecture.

In the aftermath of cyber-enabled fraud incidents, agencies and countries have established efforts at the national or even regional level to provide a response to emerging threats and offer effective solutions.

An example of a cross-sector success between governments and the financial sector in recent years is the Suspicious Activity Reports (SARs) in some of our member countries, to identify the origin of suspicious transactions that may be linked to criminal or otherwise fraudulent activity.

This effective mechanism was enabled thanks to the introduction of national legislation in concerned member countries, and it provides for cooperation between law enforcement and the financial sector.

However, this is a partial solution to a problem which deserves a global response.

In a hyper-connected world, the convergence of crime is even more evident, where industry may unwittingly play a role in the criminal chain, as private industry manages platforms that may be abused by criminal groups.

INTERPOL's vision remains clear: as the cyber threat is upon us, global law enforcement and private industry must come closer together also under a global platform that transcends national and regional efforts.

Furthermore, partnerships for enhanced cooperation between international law enforcement, telecommunications and the financial sectors should build on existing platforms for sharing information and expertise.

This was the essential message recognized by the G7 earlier in May and the G20 this past week, which calls for the "…improve[ment] of existing international information architecture in the areas of security…".

And to be successful, all sides of the table must be convinced that there is an added value to such collaboration. This is the power of having a global network, like INTERPOL, with a proven track record.

INTERPOL's Operation First Light last year targeted a variety of social engineering frauds and related financial crimes and resulted in the arrest of 1,500 people within a two-month period alone. In Spain police closed 13 call centres throughout the country which had scammed thousands of victims in Asia out of nearly 16 million euros.

In today's digital age of connectivity, most key client data and behaviour, some which may be of interest in international investigations, is held by the private sector such as the banking and telecommunications sectors.

Access to the right data from private and public partners, within agreed parameters that are mutually respected, is critical to solving criminal investigations.

The availability of relevant, actionable, and reliable information also requires that a secure platform, a new governance architecture, be in place for this critical information to be communicated and diffused to the right partners across the world, when it becomes necessary.

To be an effective deterrent to cyber-enabled criminal activity, such collaboration with industry needs to be seamless to help prevent and respond to attacks and incidents.
Information sharing and the exchange of best practices between private and public sectors is needed on a regular basis as we cannot predict when, in the future, a piece of information will be needed.

Ladies and gentlemen,
Such a global platform for information sharing exists through INTERPOL as a hub – whereby an organization has been able to secure the trust of law enforcement throughout the world.

Through our global infrastructure, we can be law enforcement's gateway to the private industry and vice versa. In this regard, the World Economic Forum has recognized INTERPOL as the only global platform enabling public-private partnerships.

It is the pace at which cyber-enabled crime is increasingly threatening our business models, our infrastructure, the stability of our economies, and most importantly, the safety of our citizens, that requires us to act faster, and more efficiently.

Through our global I-24/7 communication system, INTERPOL securely connects law enforcement in 190 member countries.

Our network serves one single operational objective: bringing relevant, actionable information to the frontlines.

Neutrality is naturally built into our infrastructure, and cooperation with law enforcement can prevail even when diplomatic relations cease to exist.

Through our operational capabilities, law enforcement agencies across the world have the ability to exchange data within a restricted environment as enshrined within our Rules on the Processing of Data that meet the highest level of international data privacy requirements.

This is underpinned through our global presence throughout the world, and our operating model that interlocks our three global crime priorities in programmes to fight terrorism, cybercrime, and organized and emerging crime.

It is also possible by speaking a common language through established and recognized standards which are the basis for effective international law enforcement cooperation. The same applies to cross-sector cooperation.

As a global standard setter, INTERPOL advocates the use of common principles to effectively exchange operational information, transcending language or regional barriers.
INTERPOL will be focusing on enhancing its role as a global standard setter to assist investigations in key areas such as biometrics and social networks.

These new standards have the potential to support international investigations and streamline requests to the financial and telecommunications industries.

Still, effectively tackling the cyber-enabled threats requires more than just establishing standards – it requires developing those experts throughout the world together with our partners.

Success in international cooperation with law enforcement and industry partners can only be ensured if we are able to 'level the playing field' and develop common goals.

To maximize the potential of collaboration, not just across sectors, but across nations and regions joint capacity building along with relevant private sector partners is a necessary part of the equation.

INTERPOL's role in this regard is also to advocate for a global, coordinated effort and be the voice for police before global fora.

We, as a global community, not just limited to law enforcement, need a harmonization of the legal frameworks at the global level that enables this seamless, secure and trusted exchange with key industry partners that paves the way for a new governance architecture.

While the challenges between the private and the public worlds still remain, we have much to gain from enhanced public-private partnerships around a common goal, with industry as a full operational partner.

Criminals will continue testing the vulnerabilities of our systems, and our tools. International legal standards will continue to evolve in respond to the threats.
The cyber element requires our cross-sector cooperation to be more targeted and strategic through a permanent cooperation between law enforcement and industry.

In my view, this means that a new governance architecture should enable a desk-by-desk approach to future cross-sector partnerships. This would allow for the deployment of both law enforcement and industry experts to respond to incidents or attacks, to mutually restore systems and allow law enforcement to gather the evidence necessary for investigative leads.

In a collective effort to stem cyber and financial crime, INTERPOL is ready to be that gateway, that bridge and interface, for a more streamlined cooperation between global law enforcement and relevant private industry partners, especially in the financial and telecommunications sectors.

Thank you.